ORIGINAL

Approved: _____
Richard Cooper
Assistant United States Attorney

Before: HONORABLE BARBARA C. MOSES
United States Magistrate Judge
Southern District of New York

DOC #

UNITED STATES OF AMERICA - v. - STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," Defendant.	**SEALED COMPLAINT** Violations of 18 U.S.C. §§ 1030(b), 1349 COUNTY OF OFFENSE: NEW YORK

16 MAG 4967

SOUTHERN DISTRICT OF NEW YORK, ss.:

Abigail Smith, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Computer Hacking Conspiracy)

1. From in or about June 2012, up to and including in or about January 2015, in the Southern District and elsewhere, STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit computer intrusion offenses in violation of Title 18, United States Code, Sections 1030(a)(2), (a)(4), (a)(5)(A), and (a)(6), to wit, LISOV provided critical online infrastructure that was used to control and/or receive stolen information from computers infected with malicious software designed to steal financial account access information, and LISOV knowingly controlled and received stolen information from such computers.

2. It was a part and an object of the conspiracy that STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and others known and unknown, would and did intentionally access computers without authorization, and

thereby would and did obtain information from protected computers, for purposes of commercial advantage and private financial gain, and in furtherance of criminal and tortious acts in violation of the Constitution and the laws of the United States, and the value of the information obtained would and did exceed $5,000, in violation of Title 18, United States Code, Section 1030(a)(2).

3. It was further a part and an object of the conspiracy that STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and others known and unknown, willfully, knowingly, and with intent to defraud, would and did access protected computers without authorization, and by means of such conduct would and did further the intended fraud and obtain anything of value, in violation of Title 18, United States Code, Section 1030(a)(4).

4. It was further a part and an object of the conspiracy that STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and others known and unknown, willfully and knowingly would and did cause the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without authorization, to protected computers, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

5. It was further a part and an object of the conspiracy that STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and others known and unknown, in transactions affecting interstate and foreign commerce, and computers used by and for the Government of the United States, willfully, knowingly, and with intent to defraud, trafficked in passwords and similar information through which computers may be accessed without authorization, in violation of Title 18, United States Code, Section 1030(a)(6).

Overt Acts

6. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. From at least in or about June 2014, a computer belonging to an individual located in Manhattan, New York was infected with malicious software known as "NeverQuest," and login credentials for online banking accounts had been stolen

from that individual's computer.

b. From at least in or about July 2013, STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, rented dedicated servers located in Germany that functioned as command and control servers for computers infected with NeverQuest malicious software (the "Germany C2 Servers").

(Title 18, United States Code, Section 1030(b), (c)(2)(B), and (c)(4)(B).)

COUNT TWO
(Conspiracy to Commit Wire Fraud)

7. From in or about June 2012 up to and including in or about January 2015, in the Southern District of New York and elsewhere, STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and others known and unknown, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343, to wit, LISOV provided critical online infrastructure that was used to control and/or receive stolen information from computers infected with malicious software designed to steal financial account access information, and LISOV knowingly controlled and received stolen information from such computers.

8. It was a part and object of the conspiracy that STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

9. I have been a Special Agent with the FBI for approximately five years. I am currently assigned to a group at the FBI's New York Field Office that is responsible, among other

things, for the investigation of cyber intrusions. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with law enforcement agents and other witnesses, and my examination of reports, records, and other evidence. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

OVERVIEW OF LISOV'S CRIMINAL SCHEME

10. From at least in or about June 2012, up to and including in or about January 2015, STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and his co-conspirators were responsible for using the NeverQuest malware, designed to infect the computers of unwitting victims and, among other things, steal their login information for financial institution accounts. LISOV and his co-conspirators then used that information to steal money from those victims via various means, including wire transfers, ATM withdrawals, and purchasing expensive goods via the Internet.

11. STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, was responsible for key aspects of the creation and administration of the botnet of computers infected with NeverQuest. LISOV maintained infrastructure for this criminal enterprise, including by renting and paying for computer servers used to administer the NeverQuest botnet. In addition to being an administrator of the NeverQuest malware, LISOV was also a user of the malware. He personally received login information from unwitting victims of the NeverQuest malware, and he sold login information and other personally identifying information of victims to other individuals on the criminal black market.

12. STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and his co-conspirators have used the NeverQuest malware to steal at least approximately $855,000 from their victims' online financial accounts, and have attempted to steal over $4 million.

BACKGROUND ON THE NEVERQUEST MALWARE

Definitions

13. Based on my training and experience, I am aware of the following:

a. **Internet Service Provider ("ISP").** An ISP is a commercial service that provides Internet connections for its subscribers. ISPs may also provide Internet email accounts and other services unique to each particular ISP.

b. **IP address.** The Internet Protocol address ("IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its sources to its destination.

c. **Instant messaging.** Instant messaging ("IM") is a collection of technologies that creates the possibility of real-time text-based communication between two or more participants via the Internet. Instant messaging allows for the immediate transmission of communications, including immediate receipt of acknowledgement or reply.

d. **Server.** A server is a centralized computer that provides services for other computers connected to it via a network or the Internet. For example, a server that is configured so that its sole task is to support a website is known simply as a "Web server." A server that only stores and processes email is known as a "mail server." The computers that use the server's services are sometimes called "clients." When a user accesses email, web pages, or files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network or Internet.

e. **Proxy.** A proxy is a computer that acts as a "middleman" for a user making indirect connections to other network services. A client computer connects to a proxy and instructs it to connect to another computer. The destination computer perceives an incoming connection from the proxy, not the client computer. Like many network services, proxies have legitimate uses, but they are often used by cyber criminals to conceal their identities and locations.

f. **Trojan.** A Trojan is malicious software, or malware, that appears to perform a desirable function for the user prior to run or install but instead facilitates the unauthorized access of the user's computer system. The NeverQuest malware is a trojan.

g. **Bot.** A bot is a computer that has been compromised by malicious software for use in completing malicious and/or illegal tasks via remote direction. Most users that have a computer acting as a bot are not aware that their computers have been compromised. A larger number of bots, called a bot network or botnet, are typically controlled by one computer called a command and control server. The owner of the command and control server can direct the botnet to, among other things, send spam, operate as proxies (blindly forwarding Internet data), or participate in other cybercrimes. The owner of the command and control server can also rent the botnet or portions thereof to other individuals.

h. **Malware.** Short for "malicious software," malware is computer software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to describe a variety of hostile or intrusive program code. Computer viruses, Trojans, and spyware are types of malware.

NeverQuest Malware

14. I have analyzed samples of NeverQuest malware and spoken with a computer scientist at the FBI who is familiar with NeverQuest malware, and I have also reviewed reports from private sector network security researchers regarding NeverQuest malware. From those sources, I have learned that NeverQuest was first observed on computer networks and infected computers in or about late 2013. NeverQuest was identified as a banking Trojan that was introduced to victim's computers through social media websites, phishing emails, or file transfers. The NeverQuest malware contained within it a database of banking and financial institutions, along with their URLs, which enabled the malware to identify banking and financial websites visited by a victim user's web browser.

15. Once surreptitiously installed on a victim's computer, NeverQuest was able to identify when a user attempted to log onto an account at a website for a financial institution. If the user visited a financial institution that NeverQuest had in its database, NeverQuest would surreptitiously insert computer code into the webpage through a "webpage injection," so that any

data entered by a user into a webpage would be communicated back to a computer server used to administer the NeverQuest malware (a "Command and Control Server", or "C2 Server").

16. NeverQuest also had the functionality to identify new banking and financial websites that were not previously in the NeverQuest database, and to update the C2 Server with that information. NeverQuest administrators would then be able to create webpage injections for those new websites, and send an update to all computers infected with NeverQuest.

17. The NeverQuest malware, once surreptitiously installed on a victim's computer, also allowed an administrator of NeverQuest to remotely control the victim's computer, and to do things such as log into the victim's banking or financial accounts.

18. Once a victim's account was compromised and a NeverQuest administrator gained access to the account, the administrator would be able to take a number of actions, including transferring money to a different account, changing login credentials, writing checks to co-conspirators and criminal accomplices, and purchasing goods from online vendors.

NEVERQUEST COMMAND AND CONTROL STRUCTURE

19. Other law enforcement agents and I have obtained documents and information from ISPs located in France and Germany, as well as forensic images of three computer servers located in Germany ("Server-1," "Server-2," and "Server-3," and collectively, the "Germany C2 Servers"). FBI computer scientists and I have reviewed the contents of those servers and associated documents and information. Based on those reviews, as described more fully below, I believe that STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, was an administrator of the NeverQuest botnet network, who rented and made available network infrastructure for the NeverQuest botnet network.

20. From my review of images of the Germany C2 Servers, and my conversations with FBI computer scientists regarding their review of the Germany C2 Servers, I believe that the Germany C2 Servers are C2 Servers for NeverQuest. The following reasons, among others, form the bases for my belief:

a. A financial institution located in the United States (the "Financial Institution") has provided Internet logs to the FBI that contain information on attempts by computers

outside of the Financial Institution to access accounts maintained with the Financial Institution. For each such attempt, those logs contain information such as the IP address from which the transmission originated, and the action that the transmission instructed the Financial Institution's computer to take. An analysis of those logs indicates that in the period from on or about November 13, 2013 to on or about June 6, 2014, numerous attempts were made by computers outside of the Financial Institution's network to access customer accounts at the Financial Institution and instruct the Financial Institution's computers to send information about the accounts to certain directories on the Germany C2 Servers. I believe that these attempts to force the Financial Institution's computers to send this information are related to the NeverQuest malware because the directories on the Germany C2 Servers to which the information was to be sent contained names that I know, based on my review of law enforcement reports and reports from private sector network security firms, to be pseudonyms for NeverQuest, such as "Catch," "Porsche," and "Smile."

b. I have identified directories on the Germany C2 Servers that received information about customer accounts described in paragraph 20(a). Those directories contain lists of financial institution account login information, including usernames and passwords.

c. Based on my training and experience, I believe that the information contained in the Financial Institution's Internet logs indicates that users of the NeverQuest malware attempted to access compromised accounts at the Financial Institution by using stolen account login credentials stored on the Germany C2 Servers.

d. In addition, the Germany C2 Servers contain numerous lists of bots, or victim computers compromised by NeverQuest, along with comments on the type of information that had been stolen from those victims. For example, I have reviewed a table listing bots by "ID number," which contains notations for each bot such as "[name of financial institution] 15k All info." Based on my training and experience, I believe that this notation indicates that the account contains $15,000 and NeverQuest has harvested all the information necessary to access and make transfers from that account.

LISOV'S PARTICIPATION IN THE NEVERQUEST SCHEME

21. Based on my review of images of the Germany C2 Servers, the contents of various emails addresses which were

obtained pursuant to search warrants issued by a United States Magistrate Judge in the Southern District of New York (the "LISOV Email Accounts"), and other evidence in this investigation, I believe that STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, controlled the Germany C2 Servers. I believe this for the following reasons, among others:

a. Server-1. For the period from on or about July 4, 2013 to on or about January 13, 2015, which includes the date when the forensic image was taken, Server-1 was registered to "Stanislav Lisov," at an address in Moscow, Russia, with a certain email address ("Email Address-1"). From my review of the contents of Email Address-1, I believe that it was used by LISOV because, among other things, (i) the email account is subscribed to by "Stanislav Lisov;" (ii) it contains emails with a PDF image of LISOV's Russian passport; and (iii) it contains emails from the online store Amazon.com discussing updates to an Amazon.com account registered to LISOV.

b. Server-1. Logs recovered from Server-1 indicate that Server-1 was accessed on a number of occasions between at least in or about December 2013 and in or about March 2014 from a certain IP address ("IP Address-1"). I believe that IP Address-1 was controlled by LISOV during this time because, among other things, documents provided by the service provider for IP Address-1 indicate that the subscriber of IP Address-1 was "Stanislav Lisov," and IP Address-1 was used to log into Email Address-1.

c. Server-2. Email Address-1 contains a confirmation email from the ISP for Server-2, which contains a root access password for Server-2. Based on my training and experience, I know that root access permits a user full access to a server, including administrative-level privileges.

22. In addition, Server-1 contains evidence that STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, in addition to being an administrator of NeverQuest C2 servers, was also a user of the NeverQuest malware. LISOV personally harvested stolen login credentials to victims' financial institution accounts, and accessed and attempted to access those accounts.

a. I have identified log files on Server-1 that list millions of login credentials, including user names, passwords, and security questions and answers, for accounts on banking and

financial websites. Certain of those log files refer to the user with the nickname "Black," who logged onto Server-1 from IP Address-1. I further believe that IP Address-1 is controlled by LISOV based on my review of documents collected from the commercial websites Amazon and Paypal because IP Address-1 was used to access accounts established by "Stanislav Lisov" on both of those websites.

b. I further believe that the users with the nicknames "Black" and "Blackf" are LISOV because in or about August 2012, the user of Email Address-1, which I believe to be LISOV, sent messages to at least two other individuals in which LISOV asked the other individuals to contact him at the address "blackf@exploit.im."

23. The Financial Institution has provided logs to law enforcement agents that reflect activity on the Financial Institution's network. Based on law enforcement's review of those logs, I have learned that those logs indicate that on or about June 6, 2014, an attempt was made by a computer outside of the Financial Institution's network to access a certain customer account at the Financial Institution (the "Victim Account"). The Victim Account belongs to an individual who, at the time, resided in Manhattan, New York (the "Victim"), and who at the time kept the Victim's personal computer in Manhattan, New York.

24. From my review of records obtained from the ISP for Server-1 (the "Service Provider"), as well as the contents of the LISOV Email Accounts, I have learned, among other things, that:

a. On or about October 21, 2014, the Service Provider notified "Stanislav Lisov," the subscriber of Server-1, that law enforcement had requested a forensic image of Server-1.

b. On or about January 13, 2015, "Stanislav Lisov" cancelled his subscription of Server-1.

LISOV TRAFFICKED IN STOLEN IDENTIFICATION INFORMATION

25. As set forth below, the LISOV Email Accounts contain numerous communications between STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and others, regarding trafficking in stolen login information and personally identifying information, the operation of malware such as NeverQuest, and using stolen login information to steal money from victims' bank accounts, among other topics.

26. From my review of preliminary English translations of Russian language emails and chats contained in Email Account-1, I have learned, among other things, that:

a. On or about June 5 and 6, 2012, LISOV exchanged messages with a co-conspirator ("CC-1"). In those messages, the following was discussed, in substance and in part:

LISOV: Hi, what are you buying now?) US bank accounts?

LISOV: hi) which banks ?

LISOV: there is BofA, I can find small ones

b. Based on my training and experience, and participation in this investigation, in the messages described above, I believe that CC-1 is a potential purchaser of stolen account information, and LISOV is asking whether CC-1 is interested in purchasing stolen login information regarding United States bank accounts. LISOV further advises CC-1 that LISOV has stolen information for Bank of America available for sale ("*there is BofA*").

c. On or about June 6, 2012, LISOV exchanged messages with CC-1. In those messages, the following was discussed, in substance and in part:

CC-1: ok, any banks with low balances. I'll specify which banks for the ones with high balances for transfers. There are mules in the US

LISOV: well look, there's BofA

860+120$ - one account

161+70 - the other one

$250+the card is linked (the balance on it is not visible

LISOV: these are the ones getting the secret questions and the main info: DOB, SSN, the card number etc.

* * *

CC-1: how much do you charge, and do you have a lot of these in general?

LISOV: 25 bucks, right at this moment I am actually sifting through the logs and checking these accounts

d. Based on my training and experience, and participation in this investigation, in the messages described above, I believe that CC-1 is advising LISOV that CC-1 has "mules," or individuals who can cash out stolen money, available to work in the United States. LISOV then advises CC-1 regarding certain Bank of America accounts for which LISOV is able to sell stolen login information, and informs CC-1 regarding the type of information available for sale ("*DOB, SSN, the card number etc.*"). When asked how much he charges for such information, LISOV informs CC-1 that he will sell the information for $25 per account.

e. On or about July 13, 2012, LISOV exchanged messages with another co-conspirator ("CC-2"). In those messages, the following was discussed, in substance and in part:

LISOV: are you still interested in logs' info?

LISOV: there is a lot of USA

f. Based on my training and experience, and participation in this investigation, in the messages described above, I believe that LISOV is asking CC-2 whether CC-2 is interested in purchasing logs containing usernames, passwords, and other login information for victims' accounts ("*logs' info*"), and that LISOV is advising CC-2 that the logs contain a number of financial accounts located in the United States ("*there is a lot of USA*").

g. On or about August 16, 2012, LISOV exchanged messages with another co-conspirator ("CC-3"). In those messages, the following was discussed, in substance and in part:

* * *

CC-3: CC needed, plus online plus ssn dob mothers maiden name and mother's date of birth. For this info I'll pay 100 dollars, if it's just cc and online - 40-50 dollars

LISOV: great I was looking for somebody who needs this info)

LISOV: I have it, will send it to you soon

LISOV: how many pieces do you need?

CC-3: I'll take everything you have

* * *

LISOV: what should be the minimum balance?

CC-3: available credit should be starting from 3k

CC-3: but check only with socks

CC-3: and clean cookies

LISOV: sure

h. Based on my training and experience, and participation in this investigation, in the messages described above, I believe that CC-3 is offering to pay LISOV anywhere between $40 and $100 for stolen credit card numbers, social security numbers, and other personally identifying information, and LISOV confirms that he has been searching for customers ("*great I was looking for somebody who needs this info*"). CC-3 advises LISOV that CC-3 only wants accounts where the available balance is $3,000, and then advises LISOV to evade detection of his efforts by checking bank accounts using proxy servers not associated with LISOV ("*check only with socks*") and to make sure that his Internet browser is cleared of "cookies" that might enable a financial institution to detect information about LISOV's location ("*and clean cookies*").

i. On or about July 9, 2012, LISOV exchanged messages with CC-3. In those messages, the following was discussed, in substance and in part:

CC-3: can you search in your botnet the cards by their first digits?

CC-3: I'll give you the first digits - you'll make a search

j. Based on my training and experience, and participation in this investigation, in the messages described above, I believe that CC-3 acknowledges that LISOV controls a botnet, and asks LISOV to search information stolen from victims in his botnet to identify certain credit cards.

k. On or about August 8, 2012, LISOV exchanged messages with CC-3. In those messages, the following was discussed, in substance and in part:

CC-3: well, and if you get any new logs, let me know

* * *

LISOV: yeah, it'll be soon, I am looking for injects, as soon as I get them there'll be new ones

l. Based on my training and experience, and participation in this investigation, in the messages described above, I believe that LISOV is advising CC-3 that he is looking for "injects," or computer code that would enable NeverQuest to harvest stolen account login information and other personally identifying information from victim computers when they access a new financial institution website. LISOV further informs CC-3 that once LISOV obtains new "injects," LISOV will be able to steal more account information ("*as soon as I get them there'll be new ones*").

m. On or about August 7, 2012, LISOV exchanged messages with another co-conspirator ("CC-4"). In those messages, the following was discussed, in substance and in part:

LISOV: do you have injects for the US? I'd like to poke around there, to experiment a bit

* * *

CC-4: thanks, yes, I do, I'll give them to you, only as soon as I install TrueCrypt

n. Based on my training and experience, and participation in this investigation, in the messages described above, I believe that LISOV is asking CC-4 whether CC-4 can

provide "injects" for financial institutions located in the United States.

o. On or about June 5, 2012, LISOV exchanged messages with another co-conspirator ("CC-5"). In those messages, the following was discussed, in substance and in part:

CC-5: tomorrow the dough is going to be transferred from the bank account into paypal

CC-5: I'll try and withdraw it

LISOV: oh

CC-5: alright, send me the BofA

CC-5: the one where there's 11K

CC-5: we have a mule

p. Based on my training and experience, and participation in this investigation, in the messages described above, I believe that CC-5 is confirming with LISOV the details of a monetary transfer out of a victim's account ("*the dough is going to be transferred from the bank account into paypal*"), and further asks LISOV to send information for a Bank of America account with an $11,000 balance ("*send me the BofA . . . the one where there's 11K*").

q. On or about January 10, 2013, LISOV exchanged messages with another co-conspirator ("CC-6"). In those messages, during which LISOV and CC-6 are discussing writing computer code to check whether stolen account information is valid, the following was discussed, in substance and in part:

LISOV: well, while I was talking to you 400 accounts got checked

CC-6: anything good?

[* * *]

LISOV: 1200 [] 5000 [] 6000 [] 5000 [] 1100

LISOV: only 2 or three accounts for 5000 each

LISOV: yes 2 accounts for 5000 and one for 600..

LISOV: I'm checking them on Thank You

[* * *]

CC-6: this is the fucking greatest [data] base - that time I could not download it normally from the server where it was stored

[* * *]

CC-6: -(I swear to God it's an ideal one

LISOV: stop hurting my heart)

LISOV: I sent it to you, go to bed, I don't wanna hear from you any more today)))

CC-6: I gave out citi cards from there for about 2 thousand for 20 bucks each

r. Based on my training and experience, and participation in this investigation, in the messages described above, I believe that LISOV is advising CC-6 that during the course of their messaging, LISOV, has validated stolen login information for 400 financial institution accounts ("*400 accounts got checked*"), and then reports on account balances for some of those accounts ("*1200 [] 5000 [] 6000 [] 5000 [] 1100*"). CC-6 compliments the quality of the database of stolen accounts, and LISOV acknowledges that he is the source of the database ("*I sent it to you, go to bed*"). CC-6 responds by advising LISOV that CC-6 sold Citibank account information for $20 per account ("*I gave out citi cards from there for about 2 thousand for 20 bucks each*").

LISOV AND OTHER CO-CONSPIRATORS USED NEVERQUEST TO STEAL MONEY FROM VICTIMS' BANK ACCOUNTS

27. From my conversations with representatives of various financial institutions and other law enforcement agents, and my review of reports and documents prepared by other agents, I believe that the NeverQuest malware has been responsible for at least approximately $4.4 million in intended financial losses, and approximately $855,000 in actual financial losses representing funds that were transferred out of victim accounts without authorization.

28. I have spoken with a representative from the Financial Institution, and from those conversations, as well as documents

provided by the Financial Institution, I have learned, among other things, that:

a. Based on an analysis of logs described in paragraph 20, analysts at the Financial Institution have identified at least approximately $685,169 in unauthorized transfers from customer accounts where the perpetrator(s) are believed to have used ```NeverQuest malware to make the attempted transfers. These attempted transfers are believed to be related to NeverQuest because either (i) the Financial Institution's computers were directed to provide information to Server-1, which, as described above, is the C2 server that STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, used to administer NeverQuest; or (ii) the Financial Institution's computers were directed to provide information to computers outside of the Financial Institution's network, and were further directed to access directories on those external computers with names that are pseudonyms for NeverQuest, such as "Catch," "Porsche," and "Smile."

b. The unauthorized transfers from accounts maintained at the Financial Institution described above were all wired to destination accounts via a bank located in Manhattan, New York.

c. Many of these transfers were identified at or near the time of the transfers as fraudulent and were reversed prior to the funds departing the destination accounts.

WHEREFORE, I respectfully request that an arrest warrant be issued for STANISLAV VITALIYEVICH LISOV, a/k/a "Black," a/k/a "Blackf," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.

Abigail Smith
Special Agent
Federal Bureau of Investigation

Sworn to before me this
5th day of August, 2016

HONORABLE BARBARA C. MOSES
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK